

Table 1. Demographic characteristics of the study population	
Age (years)	65.0 ± 10.0
Gender	
Male	50 (50.0%)
Female	50 (50.0%)
Education (years)	12.0 ± 2.0
Marital status	
Married	40 (80.0%)
Single	10 (20.0%)
Occupation	
Retired	30 (60.0%)
Unemployed	20 (40.0%)
Income (USD/month)	1000.0 ± 200.0
Health status	
Good	30 (60.0%)
Poor	20 (40.0%)
Comorbidities	
Hypertension	15 (30.0%)
Diabetes	10 (20.0%)
Cholesterol	12 (24.0%)
Smoking status	
Smoker	10 (20.0%)
Non-smoker	40 (80.0%)
Alcohol consumption	
Regular	5 (10.0%)
Occasional	15 (30.0%)
Never	30 (60.0%)
Family size	3.0 ± 1.0
Living alone	10 (20.0%)
Living with family	40 (80.0%)
Health insurance	
Yes	35 (70.0%)
No	15 (30.0%)
Medication use	
Regular	20 (40.0%)
Occasional	10 (20.0%)
Never	20 (40.0%)
Healthcare utilization	
Regular	15 (30.0%)
Occasional	10 (20.0%)
Never	25 (50.0%)
Healthcare satisfaction	
Satisfied	30 (60.0%)
Dissatisfied	20 (40.0%)
Healthcare access	
Easy	30 (60.0%)
Difficult	20 (40.0%)
Healthcare cost	
Low	20 (40.0%)
High	30 (60.0%)
Healthcare quality	
Good	25 (50.0%)
Poor	25 (50.0%)
Healthcare safety	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare effectiveness	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare equity	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare sustainability	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare innovation	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare leadership	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare governance	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare accountability	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare transparency	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare integrity	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare ethics	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare professionalism	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare collaboration	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare communication	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare partnership	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare engagement	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare empowerment	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare participation	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare inclusion	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare exclusion	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare discrimination	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare bias	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare prejudice	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare intolerance	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare hatred	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare violence	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare terrorism	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare war	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare conflict	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare aggression	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare hostility	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare animosity	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare enmity	
High	20 (40.0%)
Low	30 (60.0%)
Healthcare malice	
High	25 (50.0%)
Low	25 (50.0%)
Healthcare spite	
High	20 (40.0%)

(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

## **MULTI-LEVEL, MULTI-DIMENSIONAL CONTENT PROTECTION**

### **COPYRIGHT NOTICE**

**[0001]** A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

### **FIELD OF THE INVENTION**

**[0002]** This invention relates to digital rights management. More particularly, this invention relates to the hierarchical protection of digital content.

### **BACKGROUND OF THE INVENTION**

**[0003]** Accompanying the widespread conversion of many types of content, such as movies, music, books, etc., to digital formats has been the development of a number of systems for protecting such content against unauthorized distribution and access. In the case of digital content that is to be distributed to different environments, it is desirable to the content distributor that each environment only receive rights to the one or more attributes of the content that is appropriate to its subscriber. As used herein, an environment refers to a business model that is used by a subscriber of content for processing security rights in digital content.

**[0004]** Content may have one or more attributes, such as resolution, frame rate, number of copies, number of simultaneous users, or size of computer. The attributes that content has may depend on the type of content. For instance, video content may comprise resolution and frame rate.

**[0005]** Currently, the industry practice is to encrypt the entire contents using a single key and algorithm for distribution to all environments. Consequently, either the least secure environment will have access to the

highest resolution encoded in the content, or the content must be re-authored for each environment in accordance with the required resolution and security of that environment.

TOP SECRET

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0006]** The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

**[0007]** FIG. 1 is a block diagram illustrating multi-level and multi-dimensional hierarchical content encryption using separate keys in accordance with embodiments of the invention.

**[0008]** FIG. 2 is a block diagram illustrating a system in accordance with embodiments of the invention.

**[0009]** FIG. 3 is a block diagram illustrating hierarchical content decryption using a single key in accordance with embodiments of the invention.

**[0010]** FIG. 4 is a flowchart illustrating a method for multi-level and multi-dimensional hierarchical content encryption using separate keys in accordance with embodiments of the invention.

**[0011]** FIG. 5 is a flowchart illustrating a method for hierarchical content decryption using a single key in accordance with embodiments of the invention.

**[0012]** FIGS. 6 and 7 are matrices used for generating lower level keys in accordance with a first exemplary embodiment of the invention.

**[0013]** FIG. 8 is a matrix used for generating lower level keys in accordance with a third exemplary embodiment of the invention.

## DETAILED DESCRIPTION OF THE INVENTION

**[0014]** In one aspect of the invention, a method is provided for multi-level and multi-dimensional encoding of content for distribution to multiple environments. Content having one or more attributes is encrypted once and distributed to multiple environments having various levels of security.

**[0015]** Multi-dimensional encoding refers to encoding content that may have one or more attributes, such as resolution or frame-rate. Multi-level encoding refers to hierarchical encoding of content for a given attribute, where each successive level improves the attribute of the previous level, to achieve environment-independent encoding of content for one or more environments, where each environment has its own level of security. Both multi-dimensional encoding and multi-level encoding are characterized by the encoding of content once for distribution to multiple environments.

**[0016]** Multi-dimensional content is divided into sections. Each section is a portion of the content to be distributed, and represents a level of access for the attributes of the content, and each successive section is an improvement of the given attribute over the previous section. Each section is separately encrypted using separate keys from a hierarchy of keys. The keys of the hierarchy may be related by a cryptographic-strength one-way function, such that in decryption, the one-way function may be applied to any higher level section key to derive the key of the preceding, next lower level section.

**[0017]** For a given environment, the content is conveyed such that the highest appropriate key for the attributes and assurance of the given environment are available. The lower level keys are derived using the one-way function, so that a device for accessing the content has access to all levels less than or equal to the given key, but not greater than the given key.

**[0018]** The present invention includes various operations, which will be

described below. The operations of the present invention may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the operations. Alternatively, the operations may be performed by a combination of hardware and software.

**[0019]** The present invention may be provided as a computer program product which may include a machine-readable medium having stored thereon instructions which may be used to program a computer (or other electronic devices) to perform a process according to the present invention. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs (Compact Disc-Read Only Memories), and magneto-optical disks, ROMs (Read Only Memories), RAMs (Random Access Memories), EPROMs (Erasable Programmable Read Only Memories), EEPROMs (Electromagnetic Erasable Programmable Read Only Memories), magnetic or optical cards, flash memory, DVDs (Digital Video Discs), or other type of media / machine-readable medium suitable for storing electronic instructions.

**[0020]** Moreover, the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer (e.g., a server) to a requesting computer (e.g., a client) by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection). Accordingly, herein, a carrier wave shall be regarded as comprising a machine-readable medium.

## Introduction

**[0021]** As illustrated in FIG. 1, content 100 having a set of attributes is transformed into encrypted content 102 comprising a plurality of sections (only five sections shown) 104, 106, 108, 110, 112, where each section corresponds to one of L through N levels of access ( $L < N$ ), L being the lowest level of access

(e.g., lowest resolution), and N being the highest level of access (e.g., highest resolution). Each section is content encrypted at a level of access that a client may subscribe to. Encryption is achieved by using a plurality of hierarchically related keys 114, 116, 118, 120, 122, resulting in a plurality of dimensions 124 for a corresponding number of attributes. In preferred embodiments, the keys are related by a cryptographic-strength one-way function.

**[0022]** A method in accordance with FIG. 1 is illustrated in FIG. 4. It starts at block 400, and continues to block 402 where the hierarchical keys are generated. At block 404, encrypted content is created by applying each key to the content to create sections of the content. The method ends at block 406.

**[0023]** As illustrated in FIG. 2, a server 200 and a client 202 create a secure authenticated channel 204 that connects a digital rights management agent 208 (hereinafter "agent") on the client with a content clearinghouse 206 (hereinafter "clearinghouse") comprising content 100 on the server 200. A request to access content 100 is received from the client 202. When the server 200 receives appropriate payment from the client 202 for an M ( $L \leq M \leq N$ ) level of access, the encrypted content 102 is communicated to the client 202, along with the appropriate key for the level of access subscribed to.

**[0024]** As illustrated in FIG. 3, using a base key 300 (i.e., a key commensurate with the client's 202 subscription, or rights, which is  $K_3$  in this example), the agent 208 can create all appropriate lower level keys 302, 304. Once all appropriate keys 300, 302, 304 are obtained or created, the encrypted content 102 is decrypted into accessible content 306, where the client 202 has access to the corresponding sections 308, 310, 312 (obtained by using the appropriate key 300, 302, 304) of the content 100 having the given set of attributes less than or equal to the base key 300.

**[0025]** A method in accordance with FIG. 3 is illustrated in FIG. 5, beginning at block 500. At block 502, content having N levels of access is

received. At block 504, a base key corresponding to an M of N level of access is received, and at block 506, the base key is used to derive lower level keys for accessing content corresponding to those lower level keys. The method ends at block 508.

**[0026]** For example, consider the case where the content's given attribute is "resolution" comprising levels of access 1-5 (i.e., L through N), where 1 is the lowest resolution and 5 is the highest resolution. If a client subscribes to a mid-point resolution, say 3 (i.e., M), then upon appropriate payment, the server transmits the content along with a base key corresponding to a resolution of 3. The client then uses the base key to generate all lower level keys. Once all appropriate keys are available, corresponding sections of the content may be accessed.

**[0027]** For synchronized, multi-media applications, synchronization information is encrypted separately from the information in each synchronized channel (for example, video and audio). That is, each aspect of the multi-media content may be separately encrypted, enabling the value of each aspect to be recognized in rights management transactions. Where various aspects interact, a multi-dimensional encryption scheme can be used wherever multi-dimensional hierarchical encoding is possible. For non-interactive aspects, each may be separately protected, or, optionally, they may be artificially related for purposes of key distribution.

**[0028]** In one exemplary embodiment, a matrix for each dimension is published, such that a key with a lower subscript in each dimension can be computed from the higher value key. In another exemplary embodiment, a modular exponentiation function is utilized. In yet another embodiment, a secret sharing scheme is utilized.

Table 1. Demographic characteristics of the study population	
Age (years)	Mean (SD)
18-24	20.5 (2.5)
25-34	29.5 (4.5)
35-44	39.5 (5.5)
45-54	49.5 (6.5)
55-64	59.5 (7.5)
65-74	69.5 (8.5)
75-84	79.5 (9.5)
85-94	89.5 (10.5)
95-104	99.5 (11.5)
105-114	109.5 (12.5)
115-124	119.5 (13.5)
125-134	129.5 (14.5)
135-144	139.5 (15.5)
145-154	149.5 (16.5)
155-164	159.5 (17.5)
165-174	169.5 (18.5)
175-184	179.5 (19.5)
185-194	189.5 (20.5)
195-204	199.5 (21.5)
205-214	209.5 (22.5)
215-224	219.5 (23.5)
225-234	229.5 (24.5)
235-244	239.5 (25.5)
245-254	249.5 (26.5)
255-264	259.5 (27.5)
265-274	269.5 (28.5)
275-284	279.5 (29.5)
285-294	289.5 (30.5)
295-304	299.5 (31.5)
305-314	309.5 (32.5)
315-324	319.5 (33.5)
325-334	329.5 (34.5)
335-344	339.5 (35.5)
345-354	349.5 (36.5)
355-364	359.5 (37.5)
365-374	369.5 (38.5)
375-384	379.5 (39.5)
385-394	389.5 (40.5)
395-404	399.5 (41.5)
405-414	409.5 (42.5)
415-424	419.5 (43.5)
425-434	429.5 (44.5)
435-444	439.5 (45.5)
445-454	449.5 (46.5)
455-464	459.5 (47.5)
465-474	469.5 (48.5)
475-484	479.5 (49.5)
485-494	489.5 (50.5)
495-504	499.5 (51.5)
505-514	509.5 (52.5)
515-524	519.5 (53.5)
525-534	529.5 (54.5)
535-544	539.5 (55.5)
545-554	549.5 (56.5)
555-564	559.5 (57.5)
565-574	569.5 (58.5)
575-584	579.5 (59.5)
585-594	589.5 (60.5)
595-604	599.5 (61.5)
605-614	609.5 (62.5)
615-624	619.5 (63.5)
625-634	629.5 (64.5)
635-644	639.5 (65.5)
645-654	649.5 (66.5)
655-664	659.5 (67.5)
665-674	669.5 (68.5)
675-684	679.5 (69.5)
685-694	689.5 (70.5)
695-704	699.5 (71.5)
705-714	709.5 (72.5)
715-724	719.5 (73.5)
725-734	729.5 (74.5)
735-744	739.5 (75.5)
745-754	749.5 (76.5)
755-764	759.5 (77.5)
765-774	769.5 (78.5)
775-784	779.5 (79.5)
785-794	789.5 (80.5)
795-804	799.5 (81.5)
805-814	809.5 (82.5)
815-824	819.5 (83.5)
825-834	829.5 (84.5)
835-844	839.5 (85.5)
845-854	849.5 (86.5)
855-864	859.5 (87.5)
865-874	869.5 (88.5)
875-884	879.5 (89.5)
885-894	889.5 (90.5)
895-904	899.5 (91.5)
905-914	909.5 (92.5)
915-924	919.5 (93.5)
925-934	929.5 (94.5)
935-944	939.5 (95.5)
945-954	949.5 (96.5)
955-964	959.5 (97.5)
965-974	969.5 (98.5)
975-984	979.5 (99.5)
985-994	989.5 (100.5)
995-1004	999.5 (101.5)
1005-1014	1009.5 (102.5)
1015-1024	1019.5 (103.5)
1025-1034	1029.5 (104.5)
1035-1044	1039.5 (105.5)
1045-1054	1049.5 (106.5)
1055-1064	1059.5 (107.5)
1065-1074	1069.5 (108.5)
1075-1084	1079.5 (109.5)
1085-1094	1089.5 (110.5)
1095-1104	1099.5 (111.5)
1105-1114	1109.5 (112.5)
1115-1124	1119.5 (113.5)
1125-1134	

**[0029]** In one embodiment, a random key,  $K_{i,j}$ , is generated for each point on a D-dimensional grid, where D represents the number of attributes for given content. On the server side, content is encrypted into sections, or points on the grid, where each point is encrypted using its corresponding random key,  $K_{i,j}$ . For a dimension, X, a given matrix value in the matrix is represented by:

**[0030]**  $X_{i,j} = K_{i,j} \wedge H(K_{i+1,j}).$

**[0031]** When content is transferred to the client, a base key commensurate with the client's subscription level is transmitted, along with one or more matrices, depending upon the number of attributes there are. Using the base key, a key with a lower subscript in each dimension may be computed from a higher value key. In exemplary embodiments, an exclusive-or operation may be used to derive the lower level key. For dimension X, this may be represented as follows:

**[0032]**  $K_{i,j} = F_1(K,i,j) = X_{i,j} \wedge H(K_{i+1,j})$

**[0033]** where  $K_{i,j}$  represents the randomly generated key, which is derived from a higher-level key;  $F_1(K_{i,j})$  is the function computed by the exclusive-or of the  $X$  matrix value with the one-way function of the next highest level key  $K_{i+1,j}$  in the first dimension;  $X_{i,j}$  is the value at grid point  $(i, j)$  from the published matrix; and  $H(K_{i+1,j})$  is a one-way function of the higher level key  $K_{i+1,j}$ , such as the well-known message digest function SHA-1 or MD5, for example.

**[0034]** Similarly, for dimension Y:

**[0035]**  $K_{i,j} = F_2(K,i,j) = Y_{i,j} \wedge H(K_{i,j+1}).$

**[0036]** where  $K_{i,j}$  represents the randomly generated key, which is derived from a higher-level key;  $F_2(K_{i,j})$  is the function computed by the exclusive-or of the  $X$  matrix value with the one-way function of the next highest level key  $K_{i,j+1}$  in

the second dimension;  $Y_{i,j}$  is the value at grid point  $(i, j)$  from the published matrix; and  $H(K_{i,j+1})$  is a one-way function of the higher level key  $K_{i,j+1}$ , such as the well-known message digest function SHA-1 or MD5, for example.

**[0037]** The method can be extended to any number of dimensions. In the case of only one dimension,  $X$  can be omitted, such that:

**[0038]**  $K_i = H(K_{i+1})$

**[0039]** An example of corresponding matrices for dimensions  $X$  and  $Y$  is illustrated in FIGS. 6 and 7, where dimension  $X$  represents the attribute "frames per second", and dimension  $Y$  represents the attribute "resolution". In this example, the highest resolution and frames/second exist at grid point  $(3, 3)$ . Thus, if a client subscribes to receiving the highest level of access, the environment will receive a base key corresponding to that level.

**[0040]** As illustrated at grid point  $(3, 3)$ , it costs \$5000 to subscribe to content having the highest level resolution and the highest level of frames per second. The client for an environment subscribing to these levels receives the base key,  $K_{3,3}$ , (all keys are the same for all dimensions). The base key,  $K_{3,3}$ , may then be used to generate all lower level keys. The keys may then be used to decrypt corresponding sections of the content. In progressive, hierarchical encoding, a lower level section of the content is decoded first, and each subsequent key is used to refine the previously decoded section of the content to produce a higher level attribute.

#### *Generating Lower Level Keys*

**[0041]** Using the equation for the appropriate dimension as shown above, the agent may create keys to access lower level content by computing the lower level keys based on the base key that is transmitted to the environment.

**[0042]** Keys may be generated from dimension  $X$  (FIG. 6) as follows:



instance, since  $K_{3,3}$  is given,  $K_{3,2}$  may be computed using  $K_{3,2} = F_2(K,3,2) = Y_{3,2} \wedge H(K_{3,3})$ , and  $K_{3,1}$  may be computed by using  $K_{3,1} = F_2(K,3,1) = Y_{3,1} \wedge H(K_{3,2})$  (using "moving down" equations from matrix Y). Similarly,  $K_{2,3}$  may be computed by using  $K_{2,3} = F_1(K,2,3) = X_{2,3} \wedge H(K_{3,3})$ , and  $K_{1,3}$  may be computed by using  $K_{1,3} = F_1(K,1,3) = X_{1,3} \wedge H(K_{2,3})$  (using "moving left" equations from matrix X).

**[0058]**  $K_{2,2}$  may be computed from  $K_{2,2} = F_1(K,2,2) = X_{2,2} \wedge H(K_{3,2})$  or from  $K_{2,2} = F_2(K,2,2) = Y_{2,2} \wedge H(K_{2,3})$ .  $K_{1,2}$  may be computed from  $K_{1,2} = F_1(K,1,2) = X_{1,2} \wedge H(K_{2,2})$ , or from  $K_{1,2} = F_2(K,1,2) = Y_{1,2} \wedge H(K_{1,3})$ .  $K_{2,1}$  may be computed from  $K_{2,1} = F_1(K,2,1) = X_{2,1} \wedge H(K_{3,1})$  or from  $K_{2,1} = F_2(K,2,1) = Y_{2,1} \wedge H(K_{2,2})$ .  $K_{1,1}$  may be computed from  $K_{1,1} = F_1(K,1,1) = X_{1,1} \wedge H(K_{2,1})$  or from  $K_{1,1} = F_2(K,1,1) = Y_{1,1} \wedge H(K_{1,2})$ .

**[0059]** With this method, any path (i.e., moving left or moving down) to compute a lower value key from a higher value key produces the same result. The length of the key provided by this method is limited by the message digest that is used. For example, it would be 128 bits for MD5 and 160 bits for SHA-1.

#### Second Exemplary Embodiment

**[0060]** In another embodiment, a public modulus,  $m$ , comprising two secret large prime factors,  $p$  and  $q$ , is selected. For each dimension,  $d$ , an exponent,  $e_d$ , relatively prime to (having no common factors with)  $(p-1)*(q-1)$  is chosen. The exponents are also pair-wise relatively prime. Since the size of the group of numbers generated is relatively large, it ensures that some approaches to inverting the modular exponentiation do not work.

**[0061]** These exponents may be small, but should be greater than 3. For the maximum value of all dimensions,  $i, j, \dots$ , a secret key  $K_{i,j,\dots}$  greater than 1 and less than  $m$  is chosen.

**[0062]**  $K_{i,j,\dots}$  may then be used to encrypt the content. To form the adjacent key in dimension  $d$  when decrypting,  $K_{\dots,j,\dots}$ , from key  $K_{\dots,i+1,\dots}$ , raise it to

the  $e_d$  power mod  $m$ . An equation for this is as follows:

**[0063]**  $K_{...,i,...} = F_d(K_{...,i+1,...}) = K_{...,i+1,...}^{e_d} \text{ mod } m.$

**[0064]** Assuming  $m$  is sufficiently large to disable factoring (at least 1024 bits for most applications), it would be infeasible to reverse the computation and determine higher keys in any dimension.

**[0065]** As with the first exemplary embodiment, any path to compute a lower value key from a higher value key produces the same result. This method provides up to 1024 bits for a key.

**[0066]** Consequently, the key size, size of required information, and computation requirements may help to determine which of these two methods is optimal for a given implementation.

### Third Exemplary Embodiment

**[0067]** In yet another embodiment, a publicly known cryptographic one-way function  $H$ , and a  $d$ -dimensional secret sharing scheme  $S$  are utilized. For dimension  $d$ , key  $X_{d,i} = H(X_{d,i+1})$ . Additional artificial dimensions, such as cost, may be added to provide additional constraints. Key  $K_{i,j}... = S_n(X_{1,i}, X_{2,j}, ...)$  where  $S$  is an  $n$ -of- $n$  secret sharing scheme.

**[0068]** For example, in FIG. 8, the client may purchase a high-resolution movie encrypted with a 2 dimensional scheme, where an artificial third dimension of cost is also added. The server would communicate shares  $X_{1,3}$  and  $X_{2,3}$  to the client. The client would compute lesser value shares in each dimension using the hash function  $H$  as follows:

**[0069]**  $X_{1,2} = H(X_{1,3}), X_{1,1} = H(X_{1,2})$

**[0070]**  $X_{2,2} = H(X_{2,3}), X_{2,1} = H(X_{2,2}),$  and

**[0071]**  $X_{3,5} = H(X_{3,6}), X_{3,4} = H(X_{3,5}), X_{3,3} = H(X_{3,4}), X_{3,3} = H(X_{3,4}), X_{3,2} =$

Variable	Mean	SD	Min	Max
Age	35.5	10.5	18	65
Gender	50%	50%	Male	Female
Marital status	65%	35%	Married	Single
Education	12.5	1.5	9	16
Income	3500	1500	1000	8000
Occupation	45%	55%	Professional	Non-professional
Health status	75%	25%	Good	Poor
Smoking status	30%	70%	Smoker	Non-smoker
Alcohol consumption	15%	85%	Drinker	Non-drinker
Exercise frequency	2.5	1.5	0	5
Stress level	4.5	1.5	1	7
Sleep quality	3.5	1.5	1	7
Appetite	4.5	1.5	1	7
Energy level	4.5	1.5	1	7
Mood	4.5	1.5	1	7
Concentration	4.5	1.5	1	7
Memory	4.5	1.5	1	7
Emotional stability	4.5	1.5	1	7
Resilience	4.5	1.5	1	7
Life satisfaction	4.5	1.5	1	7
Overall health	4.5	1.5	1	7

**[0080]** In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

**[0081]** While several exemplary embodiments have been described, it should be understood by one of ordinary skill in the art that concepts of this invention are not limited to embodiments discussed herein.

Table 1. Continued	
1990-1991	1991-1992
1992-1993	1993-1994
1994-1995	1995-1996
1996-1997	1997-1998
1998-1999	1999-2000
2000-2001	2001-2002
2002-2003	2003-2004
2004-2005	2005-2006
2006-2007	2007-2008
2008-2009	2009-2010
2010-2011	2011-2012
2012-2013	2013-2014
2014-2015	2015-2016
2016-2017	2017-2018
2018-2019	2019-2020
2020-2021	2021-2022
2022-2023	2023-2024
2024-2025	2025-2026
2026-2027	2027-2028
2028-2029	2029-2030
2030-2031	2031-2032
2032-2033	2033-2034
2034-2035	2035-2036
2036-2037	2037-2038
2038-2039	2039-2040
2040-2041	2041-2042
2042-2043	2043-2044
2044-2045	2045-2046
2046-2047	2047-2048
2048-2049	2049-2050
2050-2051	2051-2052
2052-2053	2053-2054
2054-2055	2055-2056
2056-2057	2057-2058
2058-2059	2059-2060
2060-2061	2061-2062
2062-2063	2063-2064
2064-2065	2065-2066
2066-2067	2067-2068
2068-2069	2069-2070
2070-2071	2071-2072
2072-2073	2073-2074
2074-2075	2075-2076
2076-2077	2077-2078
2078-2079	2079-2080
2080-2081	2081-2082
2082-2083	2083-2084
2084-2085	2085-2086
2086-2087	2087-2088
2088-2089	2089-2090
2090-2091	2091-2092
2092-2093	2093-2094
2094-2095	2095-2096
2096-2097	2097-2098
2098-2099	2099-2100
2100-2101	2101-2102
2102-2103	2103-2104
2104-2105	2105-2106
2106-2107	2107-2108
2108-2109	2109-2110
2110-2111	2111-2112
2112-2113	2113-2114
2114-2115	2115-2116
2116-2117	2117-2118
2118-2119	2119-2120
2120-2121	2121-2122
2122-2123	2123-2124
2124-2125	2125-2126
2126-2127	2127-2128
2128-2129	2129-2130
2130-2131	2131-2132
2132-2133	2133-2134
2134-2135	2135-2136
2136-2137	2137-2138
2138-2139	2139-2140
2140-2141	2141-2142
2142-2143	2143-2144
2144-2145	2145-2146
2146-2147	2147-2148
2148-2149	2149-2150
2150-2151	2151-2152
2152-2153	2153-2154
2154-2155	2155-2156
2156-2157	2157-2158
2158-2159	2159-2160
2160-2161	2161-2162
2162-2163	2163-2164
2164-2165	2165-2166
2166-2167	2167-2168
2168-2169	2169-2170
2170-2171	2171-2172
2172-2173	2173-2174
2174-2175	2175-2176
2176-2177	2177-2178
2178-2179	2179-2180
2180-2181	2181-2182
2182-2183	2183-2184
2184-2185	2185-2186
2186-2187	2187-2188
2188-2189	2189-2190
2190-2191	2191-2192
2192-2193	2193-2194
2194-2195	2195-2196
2196-2197	2197-2198
2198-2199	2199-2200
2200-2201	2201-2202
2202-2203	2203-2204
2204-2205	2205-2206
2206-2207	2207-2208
2208-2209	2209-2